DEFENSE INFORMATION SYSTEM NETWORK (DISN)
ROUTER NETWORK SUBSCRIBER GUIDE
Version 2.0

04 December 1997

DISN Transmission Services Division
DISN Networks
Code D311

TABLE OF CONTENTS

SECTION **PAGE**

SECTION **PAGE**

SECTION **PAGE**

LIST OF FIGURES

LIST OF TABLES

SECTION 1

INTRODUCTION

1.1 PURPOSE

This document describes the services offered by the Defense Information Systems Network (DISN) router networks. The DISN continues to be described by the Office of the Secretary of Defense, Assistent Secretary of Defense for Command, Control, Communications, Computerand Intelligence (ASD C4I), 05 May 97 Memorandum to Service and agencies, as "the long haul telecommunications systems and services comprising any and all intersite voice, data, and video switching and transmission services and associated network management, to include regional services or Metropolitan Area Networks (MANs). Asynchronous transfer mode edge devices are included within the definition of long-haul

services." The DISN is also described in the *Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02A, Defense Information Systems Network (DISN) and Connected Systems, dated 22 May 1996, in accordance with the OSD definition of the DISN.*

1.2 BACKGROUND

DISN is a worldwide information transfer infrastructure supporting National Defense Command, Control, Communications, and Intelligence (C^3I) requirements as well as Corporate Information Management (CIM) and Defense Information System (DIS) areas. The DISN as described in the CJCSI 6211.02A, *Defense Information System Network and Connected Systems*, dated 22 May 1996, includes the point to point transmission, switched data services, video teleconferencing, etc. The CJCSI also directs all Services/Agencies (S/A) to submit all their long haul communications requirements to DISA for provisioning on the DISN.

The packet data portion of DISN is comprised of three router networks. The three networks are the Unclassified but Sensitive (N) Internet Protocol (IP) Router Network (NIPRNET), Secret IP Router Network (SIPRNET), and Top Secret/Sensitive Compartmented Information (TS/SCI) IP Router Network. The TS/SCI IP router network is one of several services provided by the Joint Worldwide Intelligence Communications System (JWICS) and will not be addressed in this document. The JWICS is the DISN TS network that is DIA managed, with DISA oversight and Joint Staff JS2 requirements validation (requirements/user list). JS2 validates additional nodes for JWICS. For user connections to the JWICS (non backbone), users should contact their internal Service/agency JWICS managers.
Each of the DISN router networks provides a high-speed internetworking data transport service designed to support open systems and standards. The router networks provide long-haul routing of the standard Department of Defense (DoD) IP, as mandated by the OSD. Although no other protocols will be routed by the DISN router networks, proprietary protocols can be converted or encapsulated into the DoD IP standard protocol prior to transmission.

1.3 OBJECTIVES

This document is intended for technical staff within the DoD Services and Agencies who are supporting their S/As connection to, and use of, the DISN router services. It provides an update to the existing DISN Router Network Subscriber Guide dated 14 Feb 1995 and includes a description of DISN router network subscriber services and subscriber connection requirements. Subscribers to the DISN router networks can use this document to determine how to interconnect to the network. Subscribers are strongly encouraged to transition to the DoD IP network services instead of continuing to use the X.25 protocol services in the interest of DISN performance and interoperability.

1.4 SCOPE

This document is an update to the existing DISN Router Network Subscriber Guide dated 14 Feb 1995 and supersedes it. This document has a near-term focus for describing the protocols, services and interfaces on the DISN classified and unclassified but sensitive router networks (e.g., SIPRNET, NIPRNET) . The services to be discussed in this guide are focused on providing DoD IP services.

Revisions to this document will be made as required to meet future DoD mandates.

1.5 DOCUMENT ORGANIZATION

The organization of the rest of this document is as follows. Section 2 contains a description of DISN router network services. Interface requirements are described in section 3. Section 4 contains descriptions of Transmission Control Protocol (TCP)/IP connection requirements. Section 5 describes how subscribers can support other services over the DISN router networks.

SECTION 2

DISN ROUTER SERVICE OVERVIEW

This section provides a summary description of the protocols available and services offered by the DISN router networks.

2.1 DISN ROUTER NETWORK ARCHITECTURE

Each DISN router network consists of a number of routers that are interconnected to one another with either ethernet for collocated routers or high speed serial links with line speeds varying from 64 kilobits per second to T1 rates which is 1.544 Megabits Per Second (Mbps), and up to T3 which is 45 Mbps. Those routers in each network that provide access point for subscriber connections, are referred to as the Point of Presence (POP) routers. The design goal for the maximum round trip response time across the NIPRNET or SIPRNET is less than 600 milliseconds within theater per 100 Byte packet. This time duration is measured between the source and destination NIPRNET or SIPRNET WAN routers.

The DISN data networks' router topology has been designed to provide continuous operation with network availability targeted to be at least 99.5% for any pair of single-homed systems. A world wide network management system is maintained 24 hours a day, 7 days per week. Restoral times will vary based upon location. A failed network component must be restored within 16 hours for all sites except Alaska, Panama, Spain, Turkey, Guam, Okinawa, and Japan which must be restored within 28 hours. Specifically for Singapore, a "best effort" is required for restoral times but for SIPRNET sites supporting the Global Command and Control System (GCCS), a restoral time of 6 hours is required.

The target architecture for the CONUS portion of the NIPRNET has completed an initial technology insertion to support Asynchronous Transmission Mode (ATM) between selected NIPRNET core routers at speeds from 45 to 155 Megabits per second. A technology insertion of Classified ATM Service for the SIPRNET has also been implemented. The NIPRNET Core with the CONUS Unclassified ATM Service is shown in Figure 1.

Asychronous Transfer Mode (ATM) Wide Area Networking (WAN) is state of the art technology that supports the DISN router networks. Both the Unclassified and Classified ATM Service Network Management Centers are located at the Global Operations and Security Center (GOSC), formerly referred to as the Global Control Center (GCC), on separate platforms. The DISN ATM augmentation of the NIPRNET was the implementing ATM vehicle. It consists of public ATM service network with SONET OC3 architecture and Government-owned ATM switches. The public ATM carrier provides the ATM with virtual paths. There are currently nineteen (19) Unclassified ATM Service nodes and thirty (30)

Classified ATM Service nodes. Expansion of the ATM infrastructure is an on-going process based on the requirements. The ATM extends in to the DISN Pacific theater at Wahiawa and Makalapa. DISA Code D311 is responsible for the Unclassified and Classified ATM Network Managment System.

NIPRNET CORE WITH UNCLASSIFIED DISN CONUS ATM

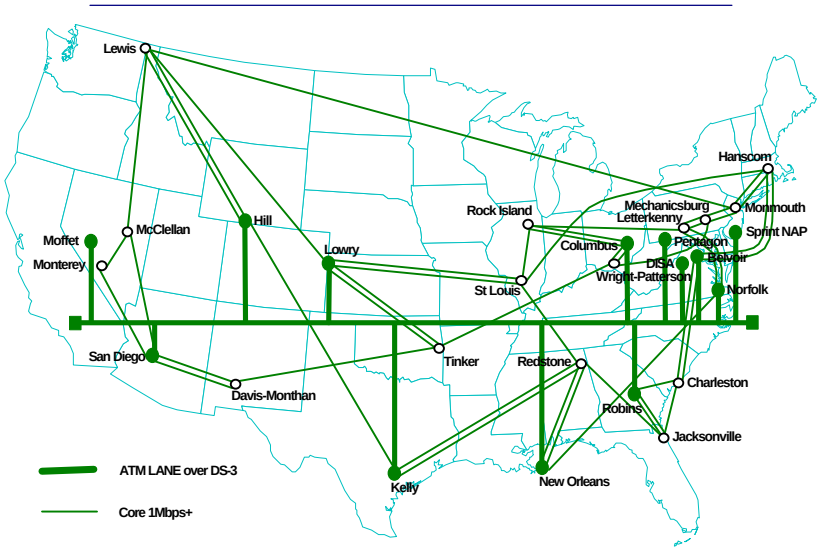

Figure 1

Specific and unique to the NIPRNET is the Joint Interconnection Service (JIS) which evolved from the former DDN Pilot Internet. The JIS services as the interconnection system for the Global NIPRNET (CONUS to OCONUS interconnections), and serves as the exit and entry points to the Federal Interconnection Exchange (FIXs). The FIXs are the two points (Network Access Point-Sprint NAP New Jersey, and FIX West Moffet Field, California) where DoD and other Federal and commercial networks interconnect to exhange routing information and provide for Global non DoD connectivity. DISA's routers at the NAP East and FIX West points are the high performance Cisco routers with T3s (45 mbps) connecting back to the JIS to support DoD to Global Internet traffic. These connection points are under constant monitoring and performance management and are upgraded in response to increases in traffic and performance requirements. DISA has also optimized the JIS with higher speed circuits and utilizing portions of the Unclassified ATM Service. The Unclassified ATM

Service has been extended to the NIPRNET Pacific theater while an additional three E1s (2.048mbps) have been implemented between NIPRNET CONUS and NIPRNET Europe theater.

2.2 DISN ROUTER SERVICES

The services offered by each DISN router network are DoD IP service. The DISN router networks service includes DISA provisioning of the access circuit for the customer's directly connected equipment (ie. customer premise router) to the DISN router network node, including associated communications equipment (ie. CSU/DSUs, encryption devices supporting the access circuit). See Section 3.2 for specific equipment and cabling requirements that must be provided by the subscriber for Ethernet accesses. Subscriber systems can use each of the DISN router networks to carry other services provided that they have been encapsulated or converted to IP before being presented to a DISN POP router.

2.2.1 DoD IP Service

TCP/IP is a layered suite of protocols. User applications use the services of TCP, which supplies a reliable, transport service. In turn, TCP uses the service of IP to deliver packets. The IP service is sometimes referred to as providing an "unreliable" service, in that it does not guarantee that packets will be in order or even arrive at their destination. Instead, it is the job of TCP to ensure that the data gets to its destination and is presented to the application in order. Between the the two end nodes can be several intervening router networks. IP routing protocols are utilized to forward the packets through the intervening networks. In the TCP/IP concept, a network could be a point-to-point serial link, a Local Area Network (LAN), or a wide area network (WAN).

The DISN DoD IP service consists of subscriber networks and hosts attached to a DISN router network. Each DISN router network (e.g., NIPRNET, SIPRNET) uses standard IP protocols to route subscriber IP data across the router network. The Cisco proprietary protocol, Interior Gateway Routing Protocol (IGRP), has been used for routing within each DISN router network. Both the NIPRNET and the SIPRNET are being transitioned to the Enhanced IGRP (EIGRP) for routing within each router network in order to implement the new security features as part of the enhanced security architecture. Both router networks utilize the Internal BGP4 to preserve Autonomous Systems (AS) associated with an advertised customer route. The IP routing protocols in use in DISN will include the Border Gateway Protocol (BGP, preferred BGP4) and the Exterior Gateway Protocol (EGP) for exterior routing protocols with subscriber systems.
The DoD Network Information Center (NIC) registers IP addresses for all DoD. Subscriber system addresses are independent of DISN router network addresses. Further discussion of addresses and protocols is included in section 4.

2.2.2 Other Services

The DISN router network currently supplies DoD IP services to subscriber hosts. In order to support other protocols, the subscriber will need to encapsulate or convert these protocols to DoD IP. Section 5 contains a description of how the subscriber can support these protocols, including X.25 and proprietary protocols (such as Systems Network Architecture (SNA)) using the DISN router networks.

2.3 TERMINAL SERVICE

The data networks (NIPRNET and SIPRNET) provide a Dial-in Data Service that allows access to the networks via dial-in asynchronous lines. The access to the data networks is provided by a Communication Server (these servers can also support terminals via dedicated connections as well). The modems associated with this service can support line speeds up to 28.8 kbps as follows: CONUS support up to 28.8kbps, Europe 14.4kpbs, Pacific theater (specifically Alaska, Guam and Hawaii) can support up to 28.8kbps dial up. 1-800 is a CONUS service only, OCONUS is local/DSN dial up. Terminal and host devices are supported. The host is a PC type device that supports the TCP/IP suite of protocols and uses the Serial Line Internet Protocol (SLIP) or the Point-to Point Protocol (PPP) to access the Communication Server. A terminal is a less sophisticated device that utilizes the TCP/IP capabilities of the Communication Server to communicate with hosts on the network. Authentication and Access control are provided by using a fixed User ID and Access Code which will be supplied to each user and which will be checked each time a user attempts to access the network (ie. NIPRNET or SIPRNET).

To access NIPRNET, each user must register with DISA via the registration process implemented at the Network Information Center (NIC). Service and agencies have a Central Registration authority identified at the NIC who orchestrates the registration process within their respective Service or agency. The registration process is documented at the NIC and can be access via the NIC Worldwide WEB. NIC services are addressed in more detail in the following sections. DISA will provide the user a Communication Server card with the user ID and access code.

For NIPRNET access, the user will be required to input the user ID and access code to the communications server for authentication and access to the network. For SIPRNET access, the dial-up access will be provided through Secure Telephone Unit III/Secure Access Control System (STU III/SACS) connected to the communication servers. Access to SIPRNET will be authenticated via the STU III/SACS, however, communication server cards will still be required to access the associated communication server.

Terminal access will also support the Point-to-Point (PPP) and the Serial Line Internet Protocol (SLIP) for systems supporting TCP/IP.

NIPRNET Dial-In Data Service

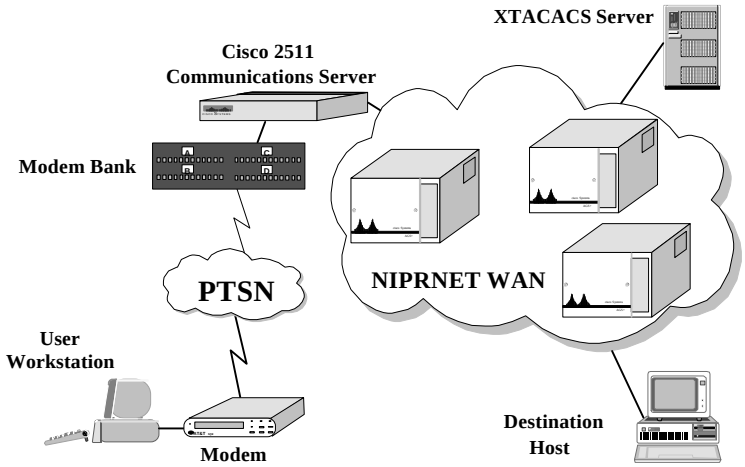

Figure 2

The NIPRNET dial-in service is depict Figure 2 above. A user at a Workstation wants to connect to a Destination Host over the NIPRNET. The user must dial into the CS over the public telephone network. The CS will request the User ID and Access Code. The User ID and Access Code will be sent to the Extended Terminal Access Controller Access Control System (XTACACS) Server by the CS for verification. The XTACACS Server will search the database for this particular User ID and Access Code. If a match is found then the user will be granted access to the NIPRNET and can then establish a connection to the Destination Host.

The SIPRNET dial-in service is depicted in Figure 3. Note that STUIII/SAC's are used instead of modems.

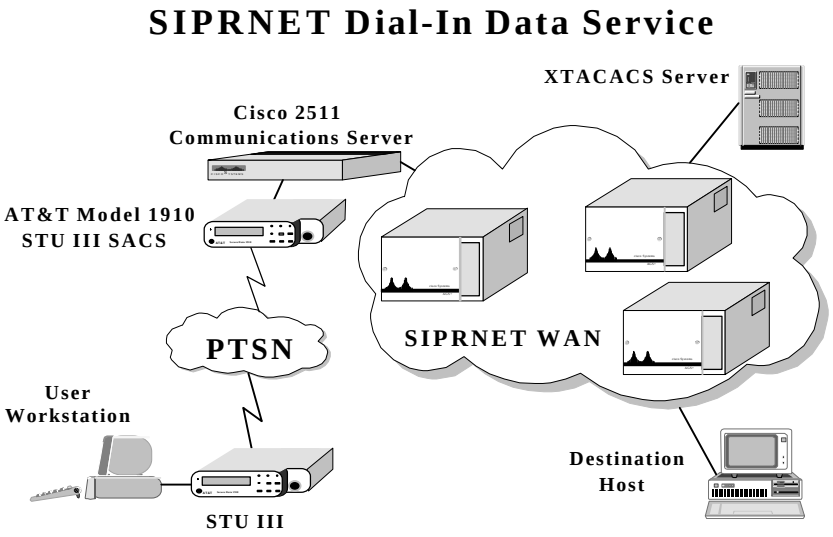

Figure 3

The dial-in data service is further described in the following documents: DISN, Dial-in Data Service, Service Description & Operational Concept, dated 25 September 1995 and DISN, Dial-in Data Service, User Guide, dated January 1996.

2.4 NETWORK INFORMATION SERVICE

2.4.1 DOD Network Information Center (NIC)

The DOD Network Information Center (NIC) is located in the Washington D.C. National Capitol Region (NCR) and is operated by DISA to provide end users of the DISN NIPRNET, a central focal point for obtaining help and information on a wide variety of network related issues and questions.

The DOD NIC performs the following functions:

-Operates registration and directory services
-Manages and administers top level and sub-level, Internet Domain Name Service (DNS) zones
-Manages, administers, and operates dial up access service support systems
-Manages the assignment and allocation of globally unique IP network address space,
-Manages the assignment of globally unique Autonomous System Numbers (ASNs)
-Maintains an on-line documentation repository of Standards, policies and general information
-Operates a world wide WEB server
-Issues Network Management Bulletins and other announcements
-Provides general user assistance via a Help Desk
-Operates the NIPRNET Security Coordination Center (SCC)

The DOD NIC for the NIPRNET provides a Help Desk that is available from 0700 to 1900 hours, Eastern Standard Time (EST), daily. CONUS subscribers call 1-800-365-3642, worldwide customers call commercial 703-802-4535. Email addresses for the NIPRNET NIC are:

hostmaster@nic.mil
Registrar@nic.mil
NIC@nic.mil
Homepage for WEB server: http://nic.mil
FTP: nic.mil
Telnet: nic.mil

The NIPRNET SCC works in conjunction with the Network Security Officer (NSO) and the Automated Systems Security Support Team (ASSIST) to:

-Coordinate actions regarding security incidents and network vulnerabilities
-Monitor use of the dial up access system and investigate possible abuse
-Issue Security Bulletins to NIPRNET users.

2.4.2 SIPRNET Support Center (SSC) Service

The SIPRNET Support Center (SSC) is located in the Washington D.C. National Capitol Region (NCR) and is operated by the Defense Information Systems Agency (DISA) to provide end users of the DISN SIPRNET, a central focal point for obtaining help and information on a wide variety of network related issues and questions.

The SIPRNET SSC performs the following functions:

-Operates registration and directory services
-Manages and administers top level and sub-level, Internet Domain Name Service (DNS) zones
-Manages, administers, and operates dial up access service support systems
-Manages the assignment and allocation of globally unique IP network address space,
-Manages the assignment of globally unique Autonomous System Numbers (ASNs)
-Maintains an on-line documentation repository of Standards, policies and general information
-Operates a world wide WEB server
-Issues Network Management Bulletins and other announcements
-Provides general user assistance via a Help Desk
-Operates the SIPRNET Security Coordination Center (SCC)

The SSC for SIPRNET provides a Help Desk that is available from 0700 to 1900 hours, EST, daily. CONUS subscribers call 1-800-582-2567, worldwide customers call commercial 703-802-8202. Email addresses for the SSC are:

hostmaster@ssc.smil.mil
Registrar@ssc.smil.mil
SSC@ssc.smil.mil
Homepage for WEB server: http://ssc.smil.mil
FTP: ssc.smil.mil
Telnet:ssc.smil.mil

The SIPRNET SCC works in conjunction with the Network Security Officer (NSO) and the Automated Systems Security Support Team (ASSIST) to:

-Coordinate actions regarding security incidents and network vulnerabilities
-Monitor use of the dial up access system and investigate possible abuse
-Issue Security Bulletins to SIPRNET users.

Unclassified email will reach the SSC by sending it to SIPRNET@NIC.MIL.

2.5 DOMAIN NAME SYSTEM

The Domain Name Seystem (DNS) provides a mechanism for mapping names to IP addresses (forward mapping) and mapping of IP addresses to names (reverse mapping). For the NIPRNET, DISA manages and administers the MIL top level domain and coordinates its release to the top level domain servers with the Global Internet. For the SIPRNET, DISA manages the root domain (MIL) and the second level SMIL domain, as well as the second level SGOV domain. Policies relating to the adminstration of the DNS for the NIPRNET and SIPRNET may be accessed electronically at the NIC and the SSC.

2.6 SUBSCRIBER SYSTEM CONNECTION METHODS

Three types of subscriber systems can be connected to each of the DISN router networks. These are local area networks with routers, local area networks without routers, and hosts (end systems). Appendix A, Planning Guidelines for Access to the Router Networks, lists types of information regarding the subscriber connection that will facilitate the installation, test and acceptance of the subscriber's access. Policies relating to the assignment and registration of IP addresses may be accessed electronically at the NIC and SSC.

2.6.1 Local Area Networks With Routers

This is the preferred option for subscriber connections to the network. The subscriber routing domain could contain multiple routers, networks, and connections. The subscriber router can be connected to a DISN POP router using any of the supported physical interfaces.
When planning a base data infrastructure, the desired configuration would be to interconnect local networks via routers. The routing structure should be such that connections to DISN are minimized to what is needed for redundancy and reliability. In the case where several networks with routers already exist, these routers should be interconnected using local resources such that the DISN router network would not be needed for traffic that both originates and terminates on base.

Subscribers are strongly advised to consider issues of performance and survivability when determining their local connectivity and the impact that connectivity will have when submitting data to the DISN router wide area networks. Subscribers are strongly encouraged to ensure their systems are not multiple layers (behind 2 or more local systems) in the local infrastructure when connecting to the DISN router networks in the interest of performance and survivability. Layering involves connecting your host/system behind/to other local systems/hosts (non NIPR/SIPR) that have direct connectivity to the long haul network (ie. NIPRNET or SIPRNET). In other words, hosts/systems directly connected to a local system do not have direct connectivity to the long haul (NIPR/SIPR) but instead, their data traffic

must first past through that local system to which they are directly connected in order to obtain wide area networking support via the NIPRNET or SIPRNET.

The subscriber will be billed for each connection to the DISN POP router. Subscribers are strongly encouraged to consider the issues of performance and survivability when considering the economics of obtaining direct or non direct (layered behind other local systems) to the DISN router networks. For further information on billing, subscribers should contact the DISN Customer Service during business hours at 1-800-554-DISN. More information on billing is provided in section 2.9.

2.6.2 Local Area Networks Without Routers

Wherever possible, subscribers are urged to connect through a router to the DISN POP router. If another organization on base already has router service, the subscriber is urged to negotiate with that organization to use a port from that router. This would ease upgrading the local service through the addition of a subscriber router at a later date.

While it is not the preferred nor optimal connection, subscriber local area networks without routers in some cases may be able to connect directly to a DISN POP router. DISN POP routers are capable of supporting Ethernet, Token Ring, and Fiber Digital Data Interface (FDDI) access. Subscriber LAN interfaces to DISN POP routers will be numbered by the authority (e.g., LAN administrator) responsible for address assignment to other entities on that LAN. This type of connectivity, when approved by DISA, is not conducive to optimizing both the local and the DISN router network performance. In these circumstances, the local systems will utilize (and compete for) valuable DISN router resources for local communications as well as for wide area communications. Therefore, DISA will allow this type of connection only in extreme and unique situations and preferably as an interim solution to meet the customer's requirements until such time the customer can obtain a customer premise router for connecting the local LAN to the DISN router network.

2.6.3 Hosts

Directly connected hosts are the least preferred option for connection to the router network. The subscriber host would connect to the DISN POP router with one of the supported serial interfaces and access the router using High-Level Data Link Control (HDLC), Link Access Procedure-Balanced (LAPB), Point-to-Point Protocol (PPP), or DDN-Standard X.25. The host must support the DoD IP.

Subscribers are urged to connect to DISN through the base or local plant, to keep service and installation support as close to the customer as possible. All issues should be considered in determining where subscribers would connect locally at the local installation. Issues of

performance, survivability, as well as economics should be carefully evaluated. Subcribers are strongly cautioned against layering more than two layers (behind other local systems) on the local installation, to obtain their wide area network connectivity from the DISN router network.

2.7 INTEROPERABILITY/APPLICATION SERVICES

DISN routers have been upgraded from the AGS+ series of CSC3s/4s processors to at least the functional equivalent of the Cisco 7000 series (ie. 7000s, 7010, 7705s, etc) to support planned security architecture enhancements. The DISN routers route IP packets using several data link layers: Ethernet**,** Token Ring, FDDI, and serial interfaces including RS-232, RS-449, and V.35. Serial interfaces may be used to interface S/A equipment with different framing to include HDLC, LAPB, PPP, and X.25.

The current TCP/IP standard application layer protocols for DISN are SMTP for electronic mail, FTP for file transfer, and TELNET for terminal access. The current OSD mandated standard applications layer protocols are DMS X.400 electronic mail and DMS X.500 Directory Services. Except for these services, any other protocols in use are not considered standard. Subscribers using non-standard protocols currently need to provide their own translation service in order to be interoperable.

2.8 SUPPORT FOR TACTICAL SYSTEMS

As part of the Integrated Tactical Strategic Data Network (ITSDN) Program, both the NIPRNET and the SIPRNET each, currently supports ten gateways globally, for connectivity to the tactical environments. These entry points are distributed worldwide. Tactical subscribers must employ TCP/IP or convert or encapsulate to IP to access DISN services. For general program information, refer to the *DISA, ITSDN Program Plan dated1994.*

DISA CONEXPLAN 10-95, which was published by DISA/D333 explains the access procedures to the ITSDN POPs in the WESTHEM. DISA-EUR's CONEXPLAN 1-96 and DISA-PAC's CONEXPLAN 203-96 explains their theater's access procedures. The following guidelines apply to accessing the ITSDN POP gateways: The ITSDN gateways are dedicated to the CINC and his component force elements during contingencies, exercises, and training missions. They are not for sustained operations. The tactical subscribers access to the ITSDN gateways is funded through the DWCF provided the requirement is validated by the appropriate CINC J6. The DISA Theater Contingency Operations Branches (D333, EU333, PC321) provide operational control and direction (via Operational Direction Message ODM) of the ITSDN gateways through the theater Regional Operations and Security Centers (ROSCs), formerly referred to as Regional Control Centers (RCCs), RSSC,

and DSCS Entry Points, etc. The customer (i.e., tactical data user), in concert with the Theater Contingency Operations Branch, will gain ITSDN gateway access only as a part of a Joint Task Force (JTF) after CINC J-6 validation.

2.9 BILLING

As a DWCF governed system, all costs to operate the DISN router network services must be offset by revenue. As a result, billing will be based upon the subscriber's fair share of the network costs which will be proportional to their requirement for network services. Bills will be based upon subscriber locations that need to be connected to the DISN and the required transmission speeds. Additional information on billing may be obtained from the annually published *Defense Working Capitol Fund (DWCF)-Communications Information Services Activity (CISA) Billing Rates for FYXX*.

Subscribers are urged to connect to DISN router networks via on-base or local network infrastructures; each physical connection to any of the DISN Router Networks will be billed. However, subscribers are strongly advised to consider issues of performance and survivability when determining their local connectivity and the impact that connectivity will have when submitting data to the DISN router wide area networks. Subscribers are strongly encouraged to ensure their systems are not multiple layers (behind 2 or more local systems) in the local infrastructure when connecting to the DISN router networks. See Section 2.6.1 for additional discussion regarding layering and performance and survivability.

The subscriber will be billed for each connection to the DISN POP router. Subscribers are strongly encouraged to consider the issues of performance and survivability when considering the economics of obtaining direct or non direct (layered behind other local systems) to the DISN router networks.

2.10 SECURITY REQUIREMENTS

Detailed security requirements are provided in the existing *DISN Security Management Plan*. Key points of the plan as they apply to subscribers of the router network are highlighted in this section.

2.10.1 DISN Router Networks Security

The DISN router networks will be protected in accordance with the *DoD Directive (DoDD) 5200.28* (series). For the NIPRNET, all routers and monitoring centers will be physically protected to the N level in CONUS; for OCONUS, the minimum level for physical protection is Secret. For dialup access to the NIPRNET, communication servers will perform Identification and Authentication (I&A) for users before allowing any access to the network.

All personnel tasked with monitoring and controlling the NIPRNET will be cleared to Secret level with a current background investigation.

For the classified networks, all circuits not contained within a protected space or protected wire distribution system have Type 1 encryption. Dial up ports for terminals will be protected by Secure Telephone Unit III/Secure Access Control System (STU III/SACS) devices. SIPRNET routers and SIPRNET monitoring centers will be protected to the Secret level. Personnel having access to the SIPRNET routers will be cleared SECRET.

Additionally, DISA plans to deploy state of the art technology during FY 97/98 to enhance the security of the network service. This technology is designed to ensure a protected network service against attacks and denial of service. The technology is using the latest advances in Fortezza and strong authentication of network management traffic, as well as protecting the networks' Regional Operations and Security Centers (ROSCs-network management centers) from external attacks by deploying Firewalls.

2.10.2 Host Requirements

For a SIPRNET access, the Automated Information Systems (AIS) (host) administrator must certify through the AIS's Designated Approving Authority (DAA) that the AIS complies with the DISN security requirements. That is, the AIS must comply with DoDD 5200.28 and undergo the mandated risk analysis and accreditation. If the attachment is not just a single host, but includes LANs and routers as well as a collection of hosts, all must comply with DoDD 5200.28 and undergo the mandated risk analysis and accreditation.

2.10.3 Network Connections

By policy, subscribers who desire connectivity to the SIPRNET must state their requirements at the time of service provisioning and their DAAs must execute a DoDD 5200.28 mandated memorandum of agreement (MOA) with the DISA DISN DAA. This policy is established through the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6211.02A, *Defense Information System Network and Connected Systems, dated 22 May 96*. Additionally, OSD/JS have delegated to DISA the authority to validate and approve contractor connections to NIPRNET. This process is documented in DISA D3 message 241049ZJUL97, Validation of Approval for Contractor Connections for NIPRNET.

It is important to note that, because of the risk that connections to external networks pose to the community at large, CJCSI 6211.02A prohibits DISN (as well as the Service/agency networks) from connecting to any non DOD element/system/network without the validation of Joint Staff, J6T, and final approval from the OSD. Additionally SIPRNET subscribers are prohibited from connecting to external networks without the approval of the DISA DISN DAA. Such connectivity is to be addressed in MOAs that are to be executed between the

external network DAA and DISA DISN DAAs. Therefore, subscribers already connected to non-DoD networks are required to supply this information at service provisioning and to execute an MOA with the DISA DISN DAA.

2.10.4 Connection Approval

An evaluation as mandated by the DISN Security Connection Approval Process (SCAP) will be conducted prior to connection of a subscriber system (host or network) to the SIPRNET. The evaluation will compare the security features of the subscriber system against a list of security objectives known as connection rules. The DISN connection rules contain requirements for documentation as well as requirements for conditional approval and full compliance. Policy and oversight of the DISN SCAP will be provided by the DISA DISN DAA.

To obtain further information on the SCAP or to start the approval process, subscribers should contact DISN Customer Services during business hours at 1-800-554-DISN.

2.10.5 Requirement for TEMPEST Countermeasures

The ASD(C3I) Memorandum, *Interim DoD Policy on the Control of Compromising Emanations*, dated 28 January 1994, establishes guidelines and procedures that will be used by DISA and S/As to determine the applicable TEMPEST countermeasures required for the DISN router network and subscriber systems.

2.10.6 DISN DAAs

DISN supports and employ security services, protection mechanisms and procedures which are based upon and reaffirm the accreditation process specified in *DoD Directive 5200.28*.

Chairman, Joint Chiefs of Staff Instruction 6211.02A, *Defense Information System Network and Connected Systems*, formed the DISN Security Accreditation Working Group (DSAWG). The DSAWG will provide, interpret, and approve DISN security policy and, under Defense Information System Security Program (DISSP) sponsorship, will make accreditation recommendations to the four designated approving authorities (DAAs) (the Directors of DISA; NSA/Chief, CSS; DIA; and the Joint Staff) for the DISN.

The DSAWG accomplishes this mission by:

a. Monitoring the life cycle of the DISN for the purpose of identifying and resolving security issues.

b. Developing and interpreting the DISN Security Policy.

c. Guiding or assisting in the development of the integrated system security architecture by ensuring consistency with the *DISN Security Policy* and the *DoD Goal Security Architecture*.

Each of the four DISN DAAs (DISA, DIA, NSA, and the Joint Staff) performs certain functions as described in the *Security Requirements for Automated Information Systems*.

2.11 DISN ROUTER NETWORK MANAGEMENT

The DISN management concept consists of three levels of management. DISA provides the centralized network monitoring via the DISA Global Operations and Security Center (GOSC), formerly referred to as the Global Control Center (GCC), and centralized network management via the DISA Regional Operations and Security Centers (ROSCs), formerly referred to as the Regional Control Centers (RCCs). DISA ROSCs support administration, operation, maintenance and status monitoring of DISN assets and services; Appendix B provides Point of Contact (POC) telephone numbers for ROSCs. Management of the subscribers' communication facilities and environment will be performed by Local Control Centers (LCCs), formerly known as Level III network management and system management centers. In most cases, the LCC facilities will be operated by the Services and Agencies, although some functions as agreed upon by the Services and Agencies and DISA may be integrated into the DISA ROSCs. Existing network management is based on the Simple Network Management Protocol (SNMP). This protocol is used for monitoring and controlling/managing the DISN routers.

Subscriber routers should support the DISN management protocol, which will initially be the Simple Network Management Protocol (SNMP). Hosts that are directly connected to DISN are required to have the capability to issue and respond to a "ping" (Internet Control Message Protocol (ICMP) Echo Request and Response).

2.11.1 Customer Premise Management

DISA Regional Operations and Security Centers (ROSCs) perform remote customer premise management for Cisco or Wellfleet routers connected directly to the NIPRNET or SIPRNET. The FY 97 fee for this service is $50.00 per month per customer router.

Premise router remote management can be obtained via submission of a Telecommunications Service Request (TSR). The customer must include in line item 401 of the TSR (Purpose of TSR--General Description), request for this service (i.e., request DISA provide customer premise management of Cisco/Wellfleet router located at...). Billing and management

services will start on the activation date shown on the Service Acquisition Message (SAM) or In-Effect Report. Premise router equipment, other than Cisco and Wellfleet, may be managed by the ROSCs only through a special Service Level Agreement (SLA) between the customers' organization and DISA.

Premise router management extends only to the premise router equipment connected directly to a NIPRNET or SIPRNET WAN/hub router. Premise router management, as depicted in Figure 4, will not extend beyond the first premise router. This means access circuits beyond the customer premise router will not be managed as part of this service.

Premise router network management services will consist of the following:

1. Router configuration table management, to include: updating and reloading, activating protocols, configuring routers, and addressing. Note: DISA will provide initial configuration of customer premise routers, for those routers that can be configured remotely.

2. Remote fault isolation and troubleshooting of the customer premise router.
3. Restoration service, across the network, of hardware equipment and software configuration. Premise router maintenance is not included in this service offering.

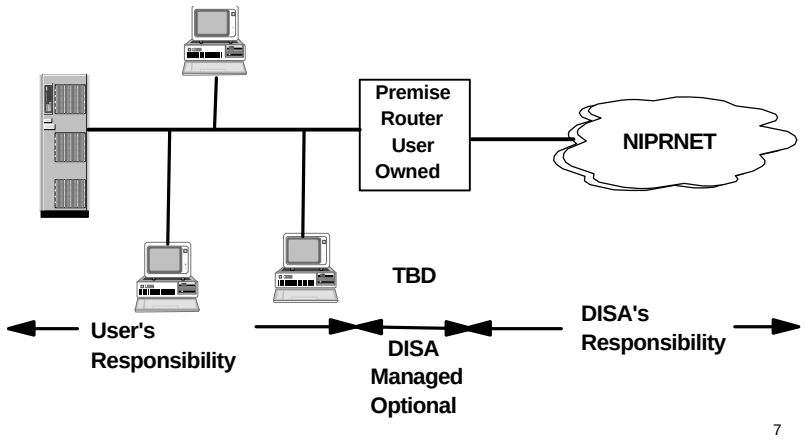

Figure 4 Network Management

It is the customers' responsibility to ensure the respective DISA ROSC receives router updates to their router configuration requirements and all premise router passwords necessary for network/configuration management. The customer must be able to provide on site personnel, at the customer premise, to aid in remote fault isolation and troubleshooting. The

respective DISA ROSC is the only authorized agent to make premise router configuration changes. Therefore, only the ROSC will have the second level password.

2.12 OBTAINING SERVICE

Service provisioning for DISN is described in DISAC 310-130-1 Supplement 12, *Defense Information System Network (DISN) Service Provisioning Procedures*. It should be noted that there may exist internal Service/agency processes for obtaining DISN router network services. These must be consistent with the OSD and JS DISN policies as discussed in this document.

Service provisioning for DISN will evolve from the current Request for Service (RFS)/Telecommunications Service Request (TSR)/Telecommunications Service Order (TSO) process with enhanced procedures and automation tools. DISA is migrating to an integrated COTS tool and database for provisioning, configuration managment and billing of DISA services. Since the DISN provisioning process is evolving, subscribers should reference the latest version of DISAC 310-130-1 Supplement 12 for current information, or access the DISA WEB site and review the DISA Catalog of Products and Services at http://www.disa.mil. Catalog descriptions of DISA services are listed under the /prodserv/listing.html. DISA is planning to provide its customers a WEB based technology and means to submit future requests for all DISA services via the existing DISA Catalog.

SECTION 3

INTERFACE REQUIREMENTS

DISN POP routers support a variety of interfaces. Some examples are provided below. The type of interface will depend on both the DISN POP router hardware version and the subscribers hardware. Subscribers should consult the *Cisco Systems Products Catalogue* or specific interface documentation provided by their vendor. The choice of interface must be specified by the subscriber at network connection provisioning request time.

3.1 SERIAL INTERFACES

The POP routers support the following synchronous serial interfaces.

- RS-530 Router Serial Interface (for 7000/7500 Series); preferred customer interface. Note that when other serial interfaces are used, converters are required. The preferred serial interface for connections to the DISN POP routers for both NIPRNET and SIPRNET.
- RS-449/422 Neighbor or Nearby Host (Data Communications Equipment (DCE) interface.
- RS-449/422 Remote Host (Data Terminal Equipment (DTE)) interface.
- RS-232 Neighbor Host (DCE) interface.
- RS-232 Remote Host (DTE) interface.
- V.35 interface.

Subscribers can use 9.6, 19.2, and 56 Kilobits per second synchronous serial service for medium-traffic requirements. For fast serial service the router will support T1 (1.544 Mbps) and E1 (2.048 Mbps) speeds as well as fractional T1 and E1 speeds. The RS-232 interface can support speeds up to 64 Kilobits per second. V.35 and RS-449 interfaces can support speeds to T1 and E1.

3.1.1 RS-232 Interface

An RS-232 interface can be used for circuits with speeds of 64 kbps or less. A DISN router can support either a DTE interface or a DCE interface. The DTE interface supplies a male 25-pin D-connector and the DCE interface a female 25-pin D-connector. Pin-outs for these

interfaces are shown in table 1.

Table 1. Synchronous RS-232 DTE Interface Pinout

Mnemonic	Pin	Signal Direction (DTE Interface)	Signal Direction (DCE Interface)
RD	**3**	**To Router**	**From Subscriber DTE device**
RC	**17**	**To Router**	**From Router**
TD	**2**	**To Subscriber DCE device**	**From Router**
TC	**15**	**To Router**	**From Router**
DTR	**20**	**To Subscriber DCE device**	**From Subscriber DTE device**
RTS	**4**	**To Subscriber DCE device**	**From Subscriber DTE device**
CTS	**5**	**To Router**	**From Router**
DCD	**8**	**To Router**	**From Router**
DSR	**6**	**To Router**	**----------**

3.1.2 RS-449 Interface

The router RS-449 interface will support speeds up to T1 or E1. Each router can support either a DTE or a DCE RS-449 interface. The DTE interface supplies a male 37-pin connector and the DCE interface supplies a female 37-pin connector.

The DISN POP router RS-449 DTE interface supplies transmit clock on Terminal Timing (TT), requiring the subscriber modem be configured to accept TT. The router interface also drives the Local Loopback (LL) signal, commanding the subscriber equipment to switch into loopback mode.

The pinouts for the RS-449 DCE interface are also shown in table 2. Subscriber equipment attached to this interface is expected to supply TT along with its data (SD). The DISN interface will respond to LL by looping signals Send Data A (SDA) and Send Data B (SDB) to signals Receive Data A (RDA) and Receive Data B (RDB).

3.1.3 V.35 DTE Interface

A DISN POP router can supply a standard V.35 connection using a rectangular, 34 pin, V.35 connector. The pin-outs are shown in table 3.

Table 2. RS-449 Interface

Mnemonic	Pin	Signal Direction (DTE Interface)	Signal Direction (DCE Interface)
Chassis ground	**1**		
SDA	**4**	**To subscriber**	**From subscriber**
SDB	**22**	**To subscriber**	**From subscriber**
STA	**5**	**To DISN POP**	**From DISN POP**
STB	**23**	**To DISN POP**	**From DISN POP**
RDA	**6**	**To DISN POP**	**From DISN POP**
RDB	**24**	**To DISN POP**	**From DISN POP**
RSA	**7**	**To Subscriber**	**From Subscriber**
RSB	**25**	**To Subscriber**	**From Subscriber**
RTA	**8**	**To DISN POP**	**From DISN POP**
RTB	**26**	**To DISN POP**	**From DISN POP**
CSA	**9**	**To DISN POP**	**From DISN POP**
CSB	**27**	**To DISN POP**	**From DISN POP**
DMA	**11**	**To DISN POP**	**From DISN POP**
DMB	**29**	**To DISN POP**	**From DISN POP**
TRA	**12**	**To Subscriber**	**From Subscriber**
TRB	**30**	**To Subscriber**	**From Subscriber**
RRA	**13**	**To DISN POP**	**From DISN POP**
RRB	**31**	**To DISN POP**	**From DISN POP**
TTA	**17**	**To subscriber**	**From Subscriber**
TTB	**35**	**To Subscriber**	**From Subscriber**
LL	**10**	**To Subscriber**	**From Subscriber**
Signal Ground	**37**		

3.2 ETHERNET

The DISN POP routers support Ethernet Version 2 and the IEEE 802.3 protocol. (Ethernet

version 2 is the proprietary standard which IEEE 802.3 is based on. The hardware is compatible, but the header formats differ slightly.) An 802.3 Media Attachment Unit (MAU) and an Attachment Unit Interface (AUI) or an Ethernet transceiver (size must not exceed size to exceed one port on the DISN router) and transceiver cable need to be supplied by the subscriber. These will connect to the Ethernet port on the back of the DISN POP router using a subscriber-supplied IEEE 802.3 AUI 15-pin slide-latch connector. Pin outs are shown in table 4.

Table 3. DISN POP V.35 DTE Interface

Pin	Signal	Direction
A	**FG**	**-**
B	**SG**	**-**
C	**RTS**	**To Subscriber**
D	**CTS**	**To DISN POP**
E	**DSR**	**To DISN POP**
F	**RLSD**	**To DISN POP**
H	**DTR**	**To Subscriber**
K	**LT**	**To Subscriber**
R	**RD+**	**To DISN POP**
T	**RD-**	**To DISN POP**
V	**SCR+**	**To DISN POP**
X	**SCR-**	**To DISN POP**
P	**SD+**	**To Subscriber**
S	**SD-**	**To Subscriber**
U	**SCTE+**	**To Subscriber**
W	**SCTE-**	**To Subscriber**
Y	**SCT+**	**To DISN POP**
a	**SCT-**	**To DISN POP**

Table 4. IEEE 802.3 AUI Pin Outs

Pin	Circuit	Description
1	**CI-S**	**Control In-Circuit Shield**
2	**CI-A**	**Control In-Circuit A**

3	**DO-A**	**Data Out-Circuit A**
4	**DI-S**	**Data In-Circuit Shield**
5	**DI-A**	**Data In-Circuit A**
6	**VC**	**Voltage Common**
9	**CI-B**	**Control In-Circuit B**
10	**DO-B**	**Data Out-Circuit B**
12	**DI-B**	**Data In-Circuit B**
13	**VP**	**Voltage Plus**
Shell	**PG**	**Protective Ground**

3.3 TOKEN RING

The DISN POP routers support 4 or 16 Mbps IEEE 802.5 or IBM-compatible Token Ring interfaces. The DISN POP Token Ring interface uses a standard DE-9 Token Ring connector, which will require a subscriber supplied Token Ring adapter cable. The pin-out for the female DE-9 connector is shown in table 5.

Table 5. DISN POP Token Ring Interface

Pin	Signal
1	**Ring Receive -**
5	**Ring Transmit -**
6	**Ring Receive +**
9	**Ring Transmit +**

3.4 FDDI

In the interest of the router network performance, DISA does not have a currently established rate/offerring for FDDI access to the DISN POP routers. However, they can support Version 6.1 of the X3T9.5 FDDI specification. This service may be offerred via the DISN POP routers at a future date depending on the requirements to do so and the enhancements that will be obtained via the DISN ATM target objective service. Specifications for the optical fiber interface are listed in table 6.

Table 6. FDDI Cables and Connectors Specification

Class A, dual-attach interface for attachment to Class A or Class B rings

FDDI standard Media Interface Connector (MIC) (connects to 62.5/125 or 50/125 micron multimode fiber optic cable)
DIN-6 connector for AMP 501916-2 Optical Bypass Switch

SECTION 4
DOD IP SERVICE

This section will describe the actions that subscribers must take to use a DISN router network IP service. Policies relating to the assignment and registration of IP addresses may be accessed electronically at the NIC and SSC.

4.1 ADDRESSING

This section will cover background information on TCP/IP addresses as well as subscriber addressing instructions.

4.1.1 IP Addresses

IP addresses are 4 octets long, and are commonly written with the decimal value of each octet, separated by periods. A host's IP address cannot have all 1's or all 0's in any field. IP addresses are assigned as class A, class B, or class C. A class A address begins with a 0 in the leftmost bit of the address and has the boundary between the net part of the address and the host part after the first octet. A class B address begins with a 10 in the leftmost two bits, and has the host address after the second octet. Class C addresses start with a 110 in the leftmost bits, and have the boundary between the net and host part of the address after the third octet. Examples are shown in figure 5.

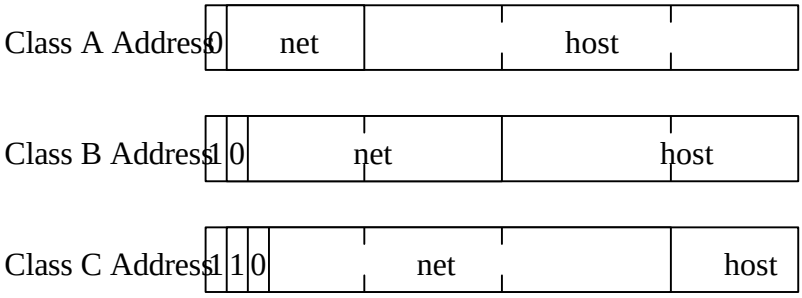

Figure 5. IP Address Examples

Subnet masks have been added to make the boundary between the net and the host more flexible than the strict boundary allowed by class A, B, or C addresses. Addresses that use subnets divide the host part of the address into a subnet part and a host part. The mask is used to separate the net and subnet portion of the address from the host portion of the address. Given the mask and address in figure 6, it can be seen that the host number is in the last 13 bits.

mask	11111111	11111111	11100000	00000000
address	10010110	00010101	11001000	00011101
network	10010110	00010101		
subnet			110	
host			01000	00011101

Recommended references for additional information on TCP/IP include *Internetworking with TCP/IP: Principles, Protocols, and Architecture*.

All DISN router networks and their segments (i.e., CONUS, Europe, Pacific) will use subnetting using fixed length and physically contiguous address masks. Subscribers systems using the DISN router networks will be required to support subnetting and use fixed length and physically contiguous address masks.

4.1.2 DISN Router Network Addressing

All the DISN router connections have distinct IP addresses. Unclassified but sensitive network's CONUS inter-router trunk links are numbered using the class A number 33 and subnet mask 255.255.255.0. Its Europe inter-router trunk links will be numbered from the class B network number 140.35 and will use the subnet mask of 255.255.255.248. Its Pacific inter-router trunk links will use the class B network number 140.45 and a subnet mask of 255.255.255.248.

SIPRNET routers are numbered using the class B number 140.49. The set of all inter-router trunk links interconnecting the SIPRNET routers will be numbered from the same IP network number space. IP subnetting will be used to assign addresses to all inter-router trunk links and interfaces.

4.1.3 Subscriber Addresses

Subscriber addresses will be assigned differently depending on whether or not there is an addressing plan in place. In either case, systems using the DISN router network will be required to support subnets using a subnet address mask with contiguous ones. Subscribers are not allowed to use physically non-contiguous addressing.

4.1.3.1 Existing Local Addressing Plan

If a subscriber has an existing LAN residing in the vicinity of a DISN POP router with direct connection to the DISN POP router, address assignments for the subscriber access link to the DISN POP router will be numbered according to the existing coordinated addressing plan. However, if such a plan does not exist or the network uses a serial link to connect to the DISN POP router, the address assignments for the subscriber access link to the DISN POP router will be assigned by the DISN router network provisioner.

4.1.3.2 No Local Addressing Plan

Where there is no local addressing plan in place, or where the link extends to a remote location that is out of scope of the existing plan, the link will be assigned an address from the DISN POP router. The request for the address(es) must be included with the service request and should include a description of the type of connection (host, LAN, or router). The

subscriber systems are numbered independently of the DISN router networks.

4.1.4 Address Registration

Subscribers should acquire addresses through their existing Service channels. Current listings of Points of Contact (POCs) for IP and DNS registrations for the unclassified (NIPRNET) are available from the DoD NIC. The DoD NIC can be contacted at NIC@NIC.MIL or 1-800-365-3642. The SIPRNET SSC can be contacted at SSC@ssc.smil.mil or 1-800-582-2567. See Sections 2.4 and 2.4.1 for additional information on the NIC and SIPRNET SSC.

4.2 PROTOCOLS

4.2.1 Address Resolution

Where the subscriber host is connected to the DISN by a serial interface, the DISN POP router will need to be configured with the subscriber's address and the subscriber will need to be configured with the DISN POP router's address. This information will need to be exchanged as part of the provisioning process.

Where the subscriber hosts are connected to the DISN POP router by a LAN, the DISN POP router will expect to perform address resolution with the ARP. An ARP query is sent to determine the data link layer address from the network address. The node corresponding to that network address responds with an ARP response indicating its data link layer address. Hosts, however, commonly need to be configured with the network layer address of at least one router. Where a subscriber LAN is connected directly to a POP router, this information will need to be exchanged as part of the provisioning process.

4.2.2 Routing

An Autonomous System (AS) is a network or collection of networks operated under a single authority running one routing protocol. An AS is required when using either EGP or BGP but not if a subscriber is using a static route to default to a single access/connection to the DISN router networks. Subscribers with multiple connections should use automated routing protocols (BGP4 is the preferred external routing protocol) and would require an AS. An interior routing protocol is run within the AS. An exterior routing protocol is run between AS's, such as between a DISN router network and the subscribers local domain (subscriber AS), to exchange routing information. Policies relating to the assignment and registration of AS numbers may be accessed electronically at the NIC and SSC.

Subscribers will need to select both interior and exterior routing methods for their networks. Subscriber hosts and LANs directly attached to the DISN POP router will not need to run any routing protocols unless they are dual-homed (In this case, dual-homed means that there are

two or more paths leaving the subscriber's AS, connected either to DISN or some other network.). For such dual-homed environments, subscriber hosts and LANs should have the capability to select the path through which each individual IP packet will be communicated. Subscriber hosts and LANs with single connection to the DISN POP router may prefer to do static routing out to the DISN POP router in the interest of local resources and local performance.

4.2.2.1 Exterior Routing

Routing between the subscribers router and the DISN POP router can be done with either static routes or, as recommended, especially for multiple connections to the DISN POP routers, through the use of the EGP, or BGP. BGP4 is the preferred protocol, but EGP will still be supported by DISN. Networks that are dual-homed to DISN can choose to use default routes, but will need to manually re-configure in the event of a failure. For dynamic re-configuration in the case of a failure, EGP or BGP should be run with the POP router. Networks with exit points other than DISN are required to run an exterior routing protocol, preferably BGP4 with the DISN.

4.2.2.2 Interior Routing

The choice of interior routing protocol, that is, the protocol run within the subscribers AS, is up to the subscriber and is independent from the protocol used for interior routing within the DISN router networks. The only case of the DISN POP router needing this information is if the subscriber desires the DISN router network to participate in the local routing protocol. This will be specified at provisioning time. DISN router networks normally use the Cisco Interior Gateway Routing Protocol (IGRP) and plans are in progress to implement the Enhanced Interior Gateway Routing Protocol (EIGRP) for routing within the router networks.
The DISN router networks also use Internal BGP4 to preserve ASs associated with an advertised customer route.

4.3 PROTOCOL TUNING AND CONFIGURATION OPTIONS

4.3.1 TCP/IP Tuning

TCP was designed to operate in the presence of errors, which can mask intermittent failures. Therefore, system or LAN administrators will benefit from monitoring the performance of the TCP/IP software. An increasing number of retransmissions may indicate an overloaded interface or a hardware problem. Logging of performance parameters may allow a host or LAN administrator to detect possible problems before they become hard failures.

Subscribers that are still running older versions of TCP should upgrade their TCP software.

Older versions may contribute to congestion by attempting too many retransmissions in an already congested network. Hosts should instead implement the improved TCP retransmission algorithms, sometimes called "Jacobson's" fixes. The use of the newer version is not only more efficient for the host, but is also more efficient for the network.

The Maximum Segment Size (MSS) and Maximum Transmission Unit (MTU) are configurable in some systems. The MTU is determined by the technology of the network to which host is attached. The MSS is a control sent to the host at the other end of the connection. In general, it is best to use the maximum setting for these values that will work. However, if these are set too large the result will be fragmentation of packets.

In most cases, subscribers should ensure that their hosts not function as a router unless it is specifically required. A host connected to only one network should never function as a router and should never run the routing protocols. A multi-homed host may or may not need to run routing protocols. In most cases, a multi-homed host should not participate in the routing protocols, but may be advantageous to listen passively. Care should be taken when configuring a multi-homed host to make sure that it does not start acting like a router and starts to handle other system's packets.

The recommendations of this section can be met if the TCP/IP implementation is consistent with *RFC 1122*.

4.3.2 Configuration Options

Configuring IP on a subscriber router will include the setting of many parameters, including setting the IP address and subnet mask for each interface and enabling or disabling various addressing options and broadcast packet handling options In addition, all the routing protocols that will be used by the router will need to be configured.

Either BGP or EGP should be run, or a default route to the POP router should be configured. If BGP or EGP is used, the subscribers should configuration their routers to identify the DISN POP routers as external neighbors. Similarly, the DISN POP router will also need to be specified as a neighbor if EGP is used. Subscribers needing assistance configuring IP on their routers should contact Customer Service during business hours at 1-800-554-DISN.

Subscribers who have attached a host or a LAN directly to a DISN POP router will also need to configure IP addresses on those hosts. Hosts on the LAN will also need to be configured to run ARP. Hosts directly attached to a DISN POP router will generally need to be configured with the address of the DISN POP router.

SECTION 5

OTHER SERVICES

The DISN router networks supply DoD IP services to subscriber hosts. Subscribers that need to support other protocols will need to encapsulate or convert these protocols to the DISN standard protocols. This section describes how the subscriber system can use the DISN router networks to support SNA and X.25 networks.

It should be noted that other DISN options are available for supporting subscriber SNA traffic, for example, connecting to the DISN Transmission Service (the multiplexer network). Subscribers are mandated by OSD and strongly encouraged by DISA to migrate to the standard IP services as soon as possible. DoD economies of scale can not be fully realized with continued support to individual proprietary networks nor can full interoperability be achieved.

5.1 SNA

Several router vendors have added capabilities to their product line to transport SNA traffic over an IP router network. The method used would depend on the configuration of the subscriber's network and on the capabilities of the subscriber routers. For transporting SNA data in the form of SDLC or LAN frames across a DISN router network, subscriber routers will be required to encapsulate the frames in IP datagrams before presentation to a DISN POP router; this will allow the DISN routers to transport the frames as normal IP network traffic. More information on this technique is provided in the following subsections. The material for this section was taken from *Integrating the Systems Network Architecture (SNA) with DISN*. Subscribers with SNA networks should also consult their vendor literature.

5.1.1 Transporting SDLC Frames

Physical Synchronous Data Link Control (SDLC) links can be replaced by a logical channel through the router network. The SDLC system on each end of the link is connected to a subscriber router port that encapsulates SDLC frames in TCP/IP packets for transmission across the router network. A similar subscriber router will receive the TCP/IP packets carrying SDLC frames, strips off the overhead associated with TCP and IP, and delivers the frames to their destination. For this encapsulation operation, these router ports are mapped to each other to provide a logical point-to-point link between the a pair of SDLC systems. The SDLC frames that are included as data within TCP/IP packets, are delivered unmodified.

Encapsulation does change some characteristics of the SDLC by adding an additional layer of control. Transport over the TCP/IP network may introduce an increase in the average delay; moreover, this delay would be variable and devices could time-out while waiting for the

acknowledgment expected from an SDLC peer. Time-outs will cause SDLC systems to retransmit frames that have already been successfully transmitted. These transmission and retransmission of SDLC poll and response frames create a large amount traffic over the router network. Additional retransmissions and time-outs will also add to transmission time of the frames.

Some methods do exist to alleviate some of the problems introduced by encapsulation. Polling, usually conducted in master-slave SDLC environments by primary systems, can be conducted instead by the encapsulation routers. In this method, known as "remote" or "proxy" polling, a router connected to secondary systems polls them on behalf of a primary system; the router connected to the primary system makes the primary system believe that the responses are coming directly from the secondary systems. This participation of routers in the polling process will eliminate the nonproductive polling and polling response SDLC frames from passing through the router network.

The above method does not, however, resolve the problem associated with the variable transmission delays and the time-out problem. Simply increasing the timer value would seriously affect performance. Other methods to compensate for these effects of TCP/IP overhead include increasing the bandwidth of the connection, assigning higher priority to encapsulation traffic, or to locally terminate the SDLC session. By locally terminating the SDLC session between an end system and the adjacent router, only frames that contain actual data will need to be transported across the router network and link-level time-outs will not occur because SDLC transmissions shall be conducted between the SDLC systems and the adjacent router.

5.1.2 Transporting LAN Frames

SNA networks supporting high speed applications may receive better performance using a LAN interconnection. Where connection of SNA devices is by token ring LANs, IBM's Source Route Bridging (SERB) and Remote Source Route Bridging (RSRB) can be used. Two or more token ring LANs can be connected to each other using RSRB over the TCP/IP router network. Each LAN would be connected through a local router that supplies the RSRB. The router network would appear to provide a virtual token-ring network. Products are available that will convert SDLC to token ring to allow the use of this method.

5.2 X.25 SERVICE

DISN packet switching layer subscribers (DDN subscribers) have been transitioned to the DISN router networks. The strategies supported to transition these subscribers included updating the host software to support a DISN standard protocol and using a subscriber-supplied router or other device to encapsulate the X.25. Subscribers are strongly encouraged to transition to the DoD IP in the interest of standardization, network performance and

interoperability.

5.2.1 DDN Standard X.25

Hosts using DDN Standard X.25 by definition use TCP/IP above X.25. Subscribers wishing to still use this service can connect either directly to the DISN POP router, or through a subscriber-provided router. In this case, the host places the IP packet inside an X.25 packet and sends it to the router, which strips off the X.25 header and routes the IP packet according to the IP address. Subscribers are urged to connect to DISN via on-base or local network infrastructures but not to be layered more than two systems/hops from the supporting DISN router providing the local base with wide area network support.

Subscribers should be cautioned that the DISN POP routers do not support all the X.25 Optional User Facilities that were supported by the DDN. The list of DDN supported Optional User Facilities that are not supported by the DISN POP routers are given in table 9.

5.2.2 DDN Basic X.25 (non SNA)

Hosts using DDN Basic X.25 by definition are using a non-TCP/IP protocol in the upper layers. Subscribers not wishing to upgrade their hosts to TCP/IP service need to supply a router to encapsulate these X.25 packets in a TCP/IP packet for presentation to the DISN router network. Since encapsulation methods are not standardized, a subscriber employing encapsulation needs to supply routers from the same manufacturer on both sides of the connection. Subscribers are cautioned to verify that their required DDN Optional User Facilities will be supported by this method. While the DISN router network will route the encapsulated IP, the end destination host must perform the same encapsulation for communication with the source host to occur (e.g., 3Com XNS to 3Com XNS).

Table 7. Unsupported X.25 Optional User Facilities

Default Throughput Class Assignment
Closed User Group w/ Outgoing Access
Closed User Group w/ Incoming Access
Incoming Calls Barred with a Closed User Group
Outgoing Calls Barred with a Closed User Group
Bilateral Closed User Group
Bilateral Closed User Group w/ Outgoing Access
Hunt Group
D-bit Modification
Closed User Group w/ Outgoing access Selection (per Call Facility)

APPENDIX A
PLANNING GUIDELINES FOR ACCESS TO THE DISN ROUTER NETWORK

The following questionnaire has been prepared to assist subscribers in preparing for the installation, test and acceptance of their DISN router network access/connection.

1. Identify customer system administrator or point of contact:
    1) Customer System POC Name: _____
    2) POC Phone: (DSN)_____ (comm)_____
    3) POC ORG/CMD_____
    4) POC Office_____
    5) POC Street Address_____
    6) City_____
    7) State_____
    8) POC AUTODIN Address_____
    9) POC Unclass E-Mail Address _____

2. Type of customer system to be connected to the DISN router network (check one):
    1) Host____
    2) Gateway/Router____
    3) Dedicated Asynchronous Terminal____
    4) Dial-In Asynchronous Terminal____
    5) Other (specify)_____

3. Host or Gateway/Router:
    1) Brand/Manufacturer_____
    2) Model_____
    3) Operating System/Software Version_____

4. Terminal Subscriber Communications Software (if any):
    1) Brand_____
    2) Version_____

5. Host, Gateway/Router, or Terminal supports (check all that apply):
    1) HDLC_____
    2) LAPB (without X.25 layer 3)_____
    3) PPP____
    4) CPPP____
    5) SLIP____
    6) CSLIP____
    7) DDN Standard X.25____
    8) DDN Basic X.25____

9) IP____
10) EGP____
11) BGP (version #)_____
12) CIDR_____

8. The DISN Data Service does not support all DDN X.25 Optional User Facilities. Does the host or gateway/router use any of the following; these are not supported by the DISN: (check all that apply)

1) Default Throughput Class Assignment_____
2) Closed User Group w/Outgoing Access_____
3) Closed User Group w/Incoming Access_____
4) Incoming Calls Barred with a Closed User Group_____
5) Outgoing Calls Barred with a Closed User Group_____
6) Bilateral Closed User Group_____
7) Bilateral Closed User Group w/Outgoing Access_____
8) Hunt Group_____
9) D-bit Modification_____
10) Closed User Group w/Outgoing Access Selection (per Call Facility)_____

9. Does the host or gateway/router support the appropriate Internet Request For Comments (RFC) for IP encapsulation in Ethernet, X.25, etc? (See Request For Comments #1720, INTERNET OFFICIAL PROTOCOL STANDARDS, November 1994 for a list of applicable protocol standards documents. Note that the STANDARDS RFC is updated quarterly.)

1) Yes_____
2) No_____

10. Does the system support remote network managment:

1) SNMP____
2) MIB (version #)____
3) Other___

1l. To facilitate troubleshooting, the DISA Regional Operations and Security Centers (ROSCs) would like read-only access to hosts and routers which are directly connected to the DISN WAN. Does the customer system agree to this arrangement?

1) Yes_____
2) No_____

12. Does the host or gateway/router support the IP class B and class C subnet addressing or variable length subnet addressing, i.e., use of subnet masks? (See Request For Comments #1720, INTERNET OFFICIAL PROTOCOL STANDARDS, November 1994 for a list of applicable protocol standards. Note that the STANDARDS RFC is updated quarterly.)

1) Class B and C Subnet Addressing____
2) Variable Length Subnet Addressing (including Classless Inter-Domain Routing, CIDR Addressing)____

13. If local networks are connected to the host or gateway/router, what internal routing (intra-domain) method is used?

1) RIP____
2) IGRP____
3) OSPF____
4) Static____
5) Other (Specify)____

14. The DISN operating policy is to use dynamic routing with BGP-4 whenever dynamic routing is required. For external routing, do you prefer to use an exterior routing protocol (inter-domain) with the DISN or do you expect to use static routing?

1) BGP (version #)____
2) EGP____
3) IS-IS (IDRP)_____
4) ES-IS_____
5) Static____
6) Other (Specify)_____

15. Do you wish to receive IP routes to all networks connected to the DISN network (NIPRNET or SIPRNET) providing your service?

1) Yes_____
2) No_____

16. Do you wish to receive routes for non-DoD/DISN networks, i.e., global Internet (NIPRNET only)?

1) Yes____
2) No_____

17. Do you wish to have DISN announce your routes to the global Internet (NIPRNET only)?

1) Yes_____
2) No_____

18. Do you have an alternate connection to the global Internet?

1) Yes_____ If yes, which connection do you plan to use as your primary path to the Internet and what routing protocol is used on the Internet connection?

DISN_____ INTERNET_____

ROUTING PROTOCOL_____

2) No_____

3) Please indicate reference for Joint Staff/OSD approval for non DOD connections as directed by policy: _____

19. Identify all IP network numbers at the local system site which need to be routed by the DISN wide-area network.

_____
_____
_____
_____
_____

APPENDIX B
POINT OF CONTACTS FOR ROSCs

1. Regional Operations and Security Centers (ROSCs)

   a. CONUS

      1. NIPRNET

         CONUS Router Monitoring Center — DSN: 850-4790/1710
         Columbus, Ohio — COMM: (800) 554-3476

      2. SIPRNET

         CONUS Router Monitoring Center — DSN: 327-4010
         Arlington, VA — COMM: (703) 607-4010
         1-800-451-7413

   b. EUROPE

      1. NIRPNET

         European Router Monitoring Center — DSN: (314) 430-5532/5534
         DISA European Area — COMM: +49-711-680-5532/5534
         Vaihingen, GE

      2. SIPRNET

         European Router Monitoring Center — DSN: (314) 430-7298/7391
         DISA European Area — COMM: +49-711-680-7298/7391
         Vaihingen, GE

   c. PACIFIC

      1. NIPRNET and SIPRNET

         Pacific Router Monitoring Center — DSN: (315) 456-1472 (EXT 105)
         DISA Pacific — COMM: (808) 656-1472 (EXT 105)
         Wheeler AAF, HI

2. Network Managers

a. CONUS

Mr. Tim Shannon	DSN:	653-8064
NIPRNET Manager	COMM:	(703) 735-8064
Mr Andrew Hogan	DSN:	364-8068
SIPRNET Manager	COMM:	(703) 735-8063

b. EUROPE (NIPRNET and SIPRNET)

MSgt Cedrick Townsend	DSN:	(314) 430-5817
NIPRNET/SIPRNET Network Manager	COMM:	+49-711-680-5817

c. PACIFIC (NIPRNET and SIPRNET)

Major Randall Bland	DSN:	(315) 456-2864
NIPRNET/SIPRNET Network Manager	COMM:	(808) 656-2864

GLOSSARY

AFB	Air Force Base
AIS	Automated Information System
ARP	Address Resolution Protocol
AS	Autonomous System
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
AUI	Attachment Unit Interface
BBN	Bolt, Beranek and Newman, Inc.
BGP	Border Gateway Protocol
C3I	Command, Control, Communications, and Intelligence
CCITT	Consultative Committee for International Telegraph and Telephone
CIM	Corporate Information Management
CIO	Central Imagery Office
CISA	Communications Information Services Activity
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CONUS	Continental United States
COTS	Commercial-Off-The-Shelf
CSU/DSU	Channel Service Unit/Data Service Units
DAA	Designated Approval Authority
DCE	Data Communications Equipment
DCO	Defense Certification Office
DCPS	Data Communications Protocol Standards
DDN	Defense Data Network
DFI	DSP Format Indicator
DIS	Defense Information System
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISSP	Defense Information System Security Program
DMS	Defense Message System
DNS	Domain Name Service
DoD	Department of Defense
DoDD	DoD Directive
DSP	Domain Specific Part
DCE	Data Circuit-Terminating Equipment
DTE	Data Terminal Equipment
DWCF	Defense Working Capitol Fund
E1	Transmission Circuit Operating at 2.048 Megabits Per Second
ECP	Engineering Change Proposals
EGP	Exterior Gateway Protocol

EIGRP	Enhanced Interior Gateway Routing Protocol
FDDI	Fiber Digital Data Interface
FOC	Full Operational Capability
FTP	File Transfer Protocol
GCC	Global Control Center
GCCS	Global Command and Control System
HDLC	High-Level Data Link Control
I&A	Identification and Authentication
ICMP	Internet Control Message Protocol
IDI	Initial Domain Identifier
IDP	Initial Domain Part
IDRP	Inter-Domain Routing Protocol
IEC	International Electrotechnical Commission
IGRP	Interior Gateway Routing Protocol
IIP	Installation/Implementation Plan Instruction
IOC	Initial Operational Capability
IP	Internet Protocol
ITSDN	Integrated Tactical Strategic Data Network
ITU-T	International Telecommunications Union - Telecommunications Standardization Sector
JCS	Joint Chiefs of Staff
JIEO	Joint Interoperability Engineering Organization
JIS	Joint Interconnection Service
Kbps	Kilobits Per Second
LAN	Local Area Network
LAPB	Link Access Procedure, Balanced
LCC	Local Control Center
LL	Local Loopback
MAU	Media Attachment Unit
Mbps	Megabits Per Second
MIC	Media Interface Connector
MOA	Memorandum of Agreement
MOP	Memorandum of Policy
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
N	Unclassified but Sensitive
NES	Network Encryption System
NET	Network Entity Titles
NIC	Network Information Center
NIPRNET	Unclssified but Sensitive IP Router Network
NSAP	Network Service Access Point
NSC	Node Site Coordinator

NVLAP	National Voluntary Laboratory Accreditation Program
OCONUS	Outside Continental United States
OSD	Office of the Secretary of Defense
OSPF	Open Shortest Path First
POC	Point of Contact
POP	Point of Presence
PPP	Point to Point Protocol
RAM	Reliability, Availability, and Maintainability
ROSC	Regional Operations and Security Center
RDA	Receive Data A
RDB	Receive Data B
RDT&E	Research, Development, Test, and Evaluation
RSRB	Remote Source Route Bridging
S/A	Service/Agency
SACS	Secure Access Control System
SDA	Send Data A
SDB	Send Data B
SDLC	Synchronous Data Link Control
SIPRNET	Secret IP Router Network
SLIP	Serial Line Internet Protocol
SMARTNET	A Cisco corporation maintenance plan
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SRB	Source Route Bridging
STU III	Secure Telephone Unit III
T1	Transmission Circuit Operating at 1.544 Megabits Per Second
TCP	Transmission Control Protocol
TS/SCI	Top Secret/Sensitive Compartmented Information
TS	Top Secret
TSO	Telecommunications Service Order
TSR	Telecommunications Service Request
TT	Terminal Timing
WAN	Wide Area Network